Root Cause Analysis Monitoring

Басель Дарвиш



Root Cause Analysis Monitoring

И как это нам всем поможет

Басель Дарвиш



Знакомимся

- PaaS и SaaS - сервисы
- Онлайн сервисы
- Состав сервиса из сервисов на Java/Spring Boot, PostgreSQL, RabbitMQ, HAproxy, и многое (очень) другое

Одна команда поддержки на несколько сервисов.

Что такое RCA

И зачем оно

Что такое RCA

Без RCA

All Active Alerts

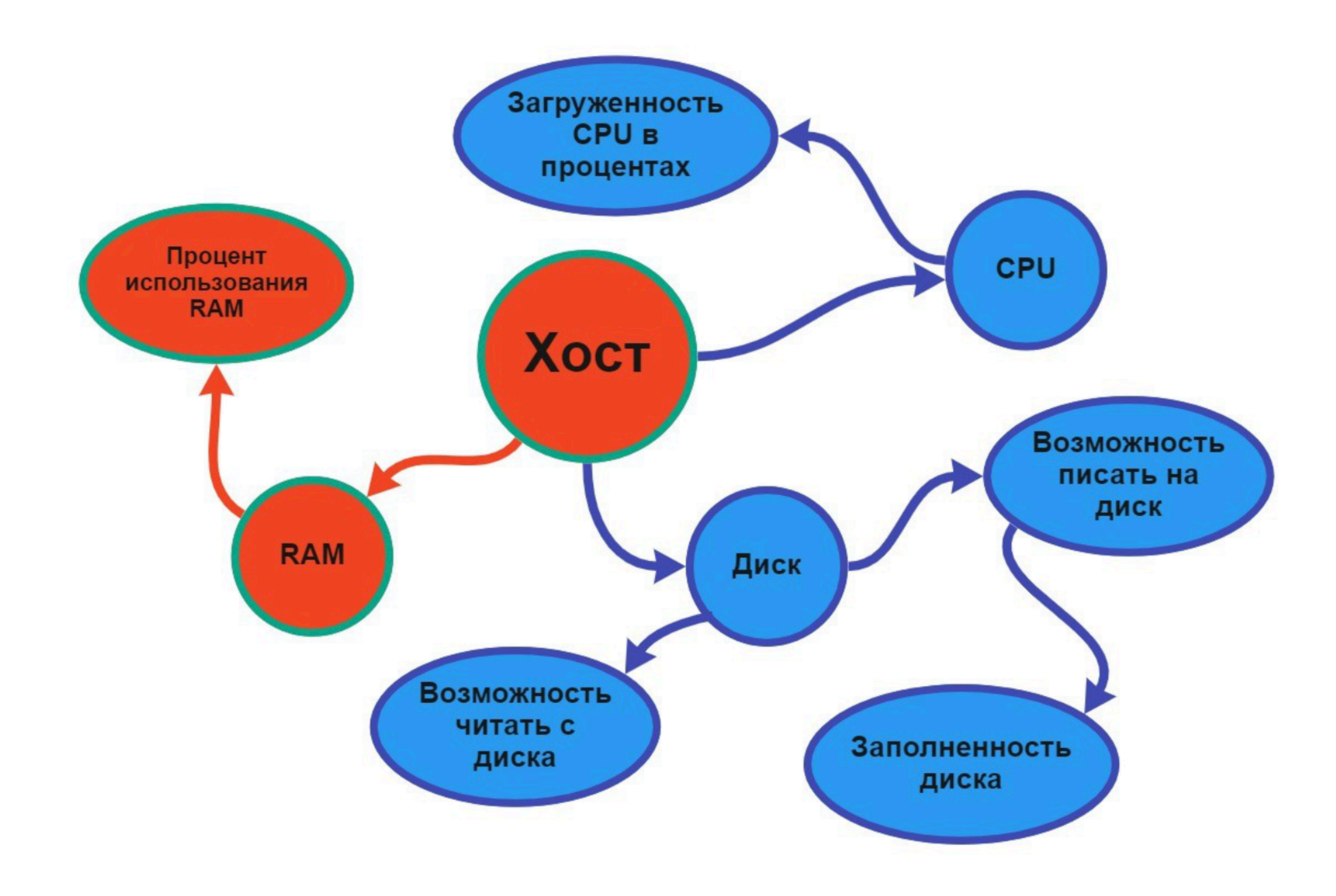
Manage Alerts | Show in NOC mode | More

ACKNOWLEDGE | VIEW ALERT DETAILS | EDIT ALERT DEFINITION | CLEAR TRIGGERED INSTANCE OF ALERT | Enter search...

Alert name	Object that triggered this alert	Active time	Trigger time
High packet loss	R1	1h 14m	1/5/2017 3:51 PM
Alert me when an application goes into warning or critical state	MSSQLSERVER on vman-2008R2-SQL	1h 19m	1/5/2017 3:46 PM
High response time	dev-brn-mkun-01	1h 49m	1/5/2017 3:16 PM
High response time	R1	2h 11m	1/5/2017 2:54 PM
High response time	R9	2h 16m	1/5/2017 2:49 PM
Alert me when an application goes down	Microsoft IIS on adf-web-21.tul.solarwinds.net	14h 14m	1/5/2017 2:51 AM
High Transmit Percent Utilization	Ethernet1 ·WAN (NetFlow) on Internet Gateway 3725	16h 58m	1/5/2017 12:07 AM
Alert me when a transaction step goes into warning or critical state	Sign in to Office 365	1d 8h 58m	1/4/2017 8:07 AM
Alert me when a transaction goes into warning or critical state	Office 365 from Austin	1d 8h 58m	1/4/2017 8:07 AM
Alert me when an application goes down	Microsoft IIS on ADF-WEB-03	1d 12h 56m	1/4/2017 4:09 AM
Alert me when a transaction step goes down	Microsoft Dynamics CRM Online	1d 13h 44m	1/4/2017 3:21 AM
Alert me when a transaction step goes down	Log out from Office 365	1d 14h 24m	1/4/2017 2:41 AM
Host memory utilization	LAB-DEM-HYV on lab-dem-hyv.demo.lab	1d 15h 25m	1/4/2017 1:39 AM
Host CPU utilization	SYD-HYV-02 on 10.199.5.109	1d 15h 25m	1/4/2017 1:39 AM
Host CPU utilization	bas-esx-02.lab.tex	1d 15h 25m	1/4/2017 1:39 AM
Host CPU utilization	tok-esx-02.lab.tex	1d 15h 25m	1/4/2017 1:39 AM
Alert me when a transaction step goes down	Navigate to email section	1d 16h 14m	1/4/2017 12:51 AM
NTA: CBQoS Drops	QoS-Ethernet-Shaper\class-default\QoS-WAN-Ethernet\Web	1d 16h 42m	1/4/2017 12:23 AM
Alert me when a component goes into warning or critical state	Top Indexes for Database (dnn) on LAB-DEM-SQL-02	1d 21h 23m	1/3/2017 7:42 PM
NTA: CBQoS Drops	QoS-Ethernet-Shaper\class-default (Drops)	1d 21h 42m	1/3/2017 7:23 PM
Page me when a Node goes down(2)	Lab/ Samsung	1d 22h 37m	1/3/2017 6:28 PM

Что такое RCA

С RCA



Окружение

- ~1000+ алертов при аварии и поломках
- ~2000000 объектов мониторинга на администратора
- Команда администраторов
- Очень много клиентов

Кому нужен мониторинг

- Администраторам

Кому нужен мониторинг

- Администраторам
- Поддержке

Кому нужен мониторинг

- Администраторам
- Поддержке
- Пользователям

Observability


Уведомления
Наглядный просмотр данных
Отладка
Профилирование
Анализ зависимостей
Предотвращение проблемы в будущем
Мониторинг
Наблюдаемость (Observability)

2.
Что мониторим

Инфраструктуру, сервисы, бизнес логику — все

Объекты мониторинга

Инфраструктура

Хосты, роутеры, диски (доступность на чтение/запись, скорость, другие показатели), состояние оборудования, сетевая связность.

Объекты мониторинга

Инфраструктура

Хосты, роутеры, диски (доступность на чтение/запись, скорость, другие показатели), состояние оборудования, сетевая связность.

Сервисы и процессы

Состояние процессов, их доступность, поток логов, работа СУБД, функций ОС, доступность по портам/проч.

Объекты мониторинга

Инфраструктура

Хосты, роутеры, диски (доступность на чтение/запись, скорость, другие показатели), состояние оборудования, сетевая связность.

Сервисы и процессы

Состояние процессов, их доступность, поток логов, работа СУБД, функций ОС, доступность по портам/проч.

Бизнес-функции

Возможность размещения заказов, состояние очередей, критичных для выполнения бизнес-функций, связанность с конкретными внешними зависимостями и т.д.

Root Cause Analysis Monitoring

- **Все объекты** на графе зависимостей

Root Cause Analysis Monitoring

- Все объекты на графе зависимостей
- Все слои **проинтегрированы** в мониторинге

Root Cause Analysis Monitoring

- Все объекты на графе зависимостей
- Все слои проинтегрированы в мониторинге
- На **одном интерфейсе** администрирования

1


администратор


~2 000 000


объектов мониторинга

3.
Соберем свой сервис


Архитектура и немного деталей

Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Сервис визуального отображения
Источники телеметрии


1
Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Сервис визуального отображения
Источники телеметрии



Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
2
Мессенджеры
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Сервис визуального отображения
Источники телеметрии

Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинг
Мессенджеры
Графовая БД (Neo4j)
3
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Сервис визуального отображения
Источники телеметрии


Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
БД временных
рядов
rometheus)
Система оповещений
Сервис RCA
4
Администратор
Сервис визуального отображения
Источ ики телеметрии


Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
5
Система оповещений
Сервис RCA
Администратор
Источники телеметрии
Сервис визуального отображения


Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Сервис визуального отображения
Источники телеметрии
5.5


Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Сервис визуального отображения
ники телеметрии
6



Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
Система оповещений
7
рвис RCA
Администратор
Источники телеметрии
Сервис визуального отображения

Сервис регистрации источников телеметрии

- Bash -> Java, Sprint Boot
- Идемпотентный Restful API

Источники телеметрии (exporter) создаются и удаляются — нам надо, чтобы сервис сбора Prometheus знал, откуда ее брать.

Пример запроса

```
{
    //...
    "name": "some-service-exporter",
    "addr": [
        "https://192.168.12.23:9090"
    ],
    "interval": 60 // Частота опрос в секундах
    //...
}
```

Пример файла конфигурации Prometheus

```
#...

  - job_name: some-service-exporter
    honor_timestamps: true
    scrape_interval: 60s
    metrics_path: /metrics
    scheme: https
    static_configs:
      - targets: [192.168.12.23:9090]

#...
```

Сервис регистрации объектов мониторинга

- Bash -> Java, Sprint Boot
- Идемпотентный Restful API
- Регистрируем объект и то, от чего он зависит
- Определиться, будет ли регистрация — mission critical-функцией

Этот сервис может оказаться нагруженным в большой и динамической инфраструктуре.

Пример запроса

```
{
    //...
    "targetId": "target-no-1",
    "severity": "low",
    "config": {
        "prom_alert_expr": "up{application_id=\"00000000-0000-0000-0000-000000000000\"}",
        "prom_alert_duration": "30s"
    },
    "dependencies": [
        "master-target-1",
        "master-target-2"
    ]
    //...
}
```

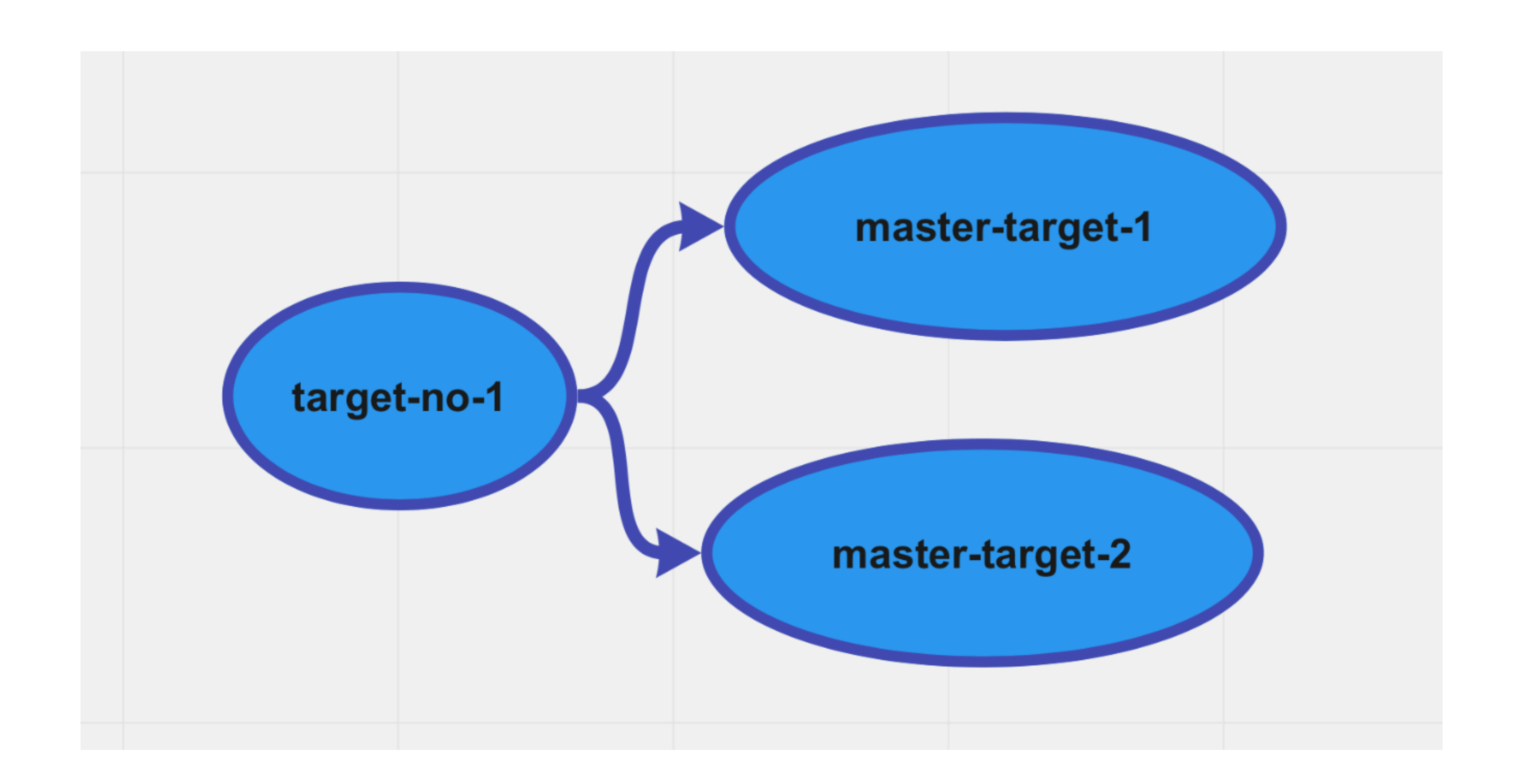
Пример конфигурации файла Prometheus

```
#...

- alert: target-no-1
  expr: node_filesystem_readonly{mountpoint='/',host_id='host1.lan'} == 1
  for: 5m
  labels:
    targetId: target-no-1
- alert: target-no-2
  expr: up{application_id=\"00000000-0000-0000-0000-000000000000\"}
  for: 30s
  labels:
    targetId: target-no-2

#...
```

Пример наполнения Neo4j



RCA Service

- Python -> Java, Sprint Boot
- GraphQL API
- По любому объекту достаем граф upstream- и downstream-зависимостей

Сервис анализирует все возведенные уведомления по объектам и работает с сервисом уведомлений.

Notifications Service

- Нотификации
- Учитывает **Severity** объектов
- Уведомляет с учетом Severity всех связанных возведенных объектов

Пример нотификаций

[FIRING:1] host-[redacted] (target_alerts 127.0.0.1:6969 rca low host-ng-link[redacted]
RootCause:
target_alerts : rca - host-ng-[redacted]
Affected:

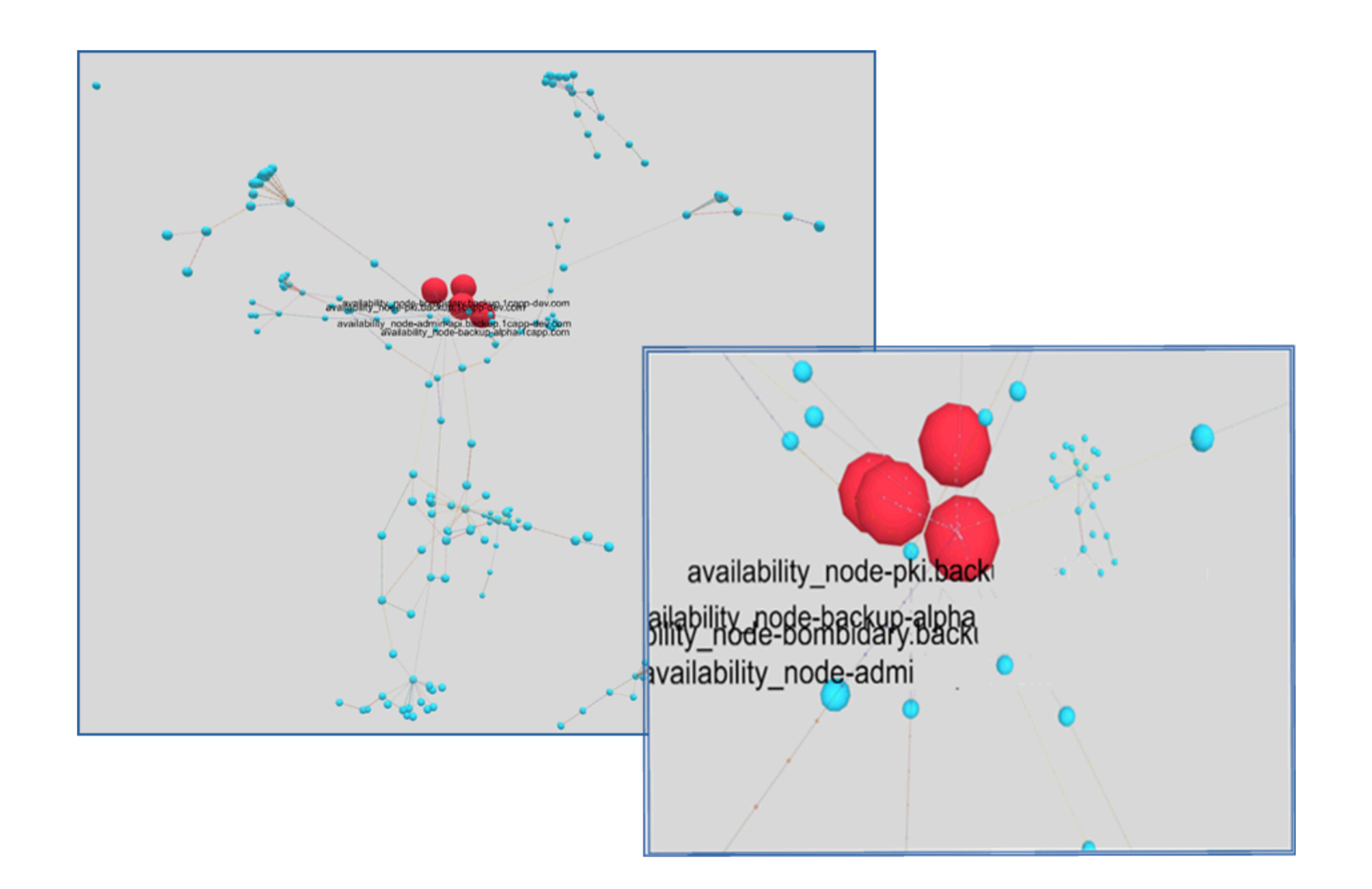
[FIRING:3] lb_1c-ha[redacted] (target_alerts 127.0.0.1:6969 rca low)
RootCause:
target_alerts : rca - lb_1c-haproxy-n[redacted]
Affected:
target_alerts : rca - lb_1c[redacted]
target_alerts : rca - lb_1c[redacted]

Prometheus

- Сбор телеметрии
- Обработка алертов
- Дополнительно — можно использовать сервис уведомлений


Сервис отображения


- 3d-force-graph
- Выделяем проблемные объекты
- Можно интегрировать с свои дэшборды, например, на базе Grafana


availability_node-backup-alpha.1capp.com
availability_node-pki.back
ailability_node-backup-alpha
bility_node-bombidary.back
availability_node-admi


4.
Встраиваем в процессы

С особенностями

1
Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Сервис визуального отображения
Источники телеметрии


Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
2
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Источники телеметрии
Сервис визуального отображения


Сервис
регистр
источн
3
Сервис регистрации объектов мониторинга
Мессенджеры
рафовая БД (Neo4j)
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Сервис визуального отображения
Источники телеметрии

Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
4
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Сервис визуального отображения
Источники телеметрии



Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
5
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Источники телеметрии
Сервис визуального отображения


Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Источники телеметрии
6


Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
7
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
Источники телеметрии
Сервис визуального отображения


Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
Систем
оповещен
8
Сервис RCA
Администратор
Сервис визуального отображения
Источники телеметрии


Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
9
Система оповещений
Сервис RCA
Администратор
Сервис визуального отображения
Источники телеметрии



Сервис регистрации источников телеметрии
Сервис регистрации объектов мониторинга
Мессенджеры
Графовая БД (Neo4j)
БД временных рядов (Prometheus)
Система оповещений
Сервис RCA
Администратор
10
Сервис визуального отображения
Источники телеметрии

Интегрируем в процессы создания объектов

Процесс должен быть очень простым.

Например, функция на Saltstack для init и для absent. Или хуки в K8s.

Интегрируем в процессы обновления объектов

Процесс должен быть очень простым.

Например, функция на SaltStack для init и для absent.

Обновление = создание.

Интегрируем в процессы удаления объектов

Нельзя недооценивать этот пункт.

Удалять — сложно, особенно при авариях.

Ложные срабатывания — главный враг.

4.1. Приоритеты

Используем RCA, чтобы не “дергаться”

Примечание

Критичность относительна

Критичность объекта

Объект вне графа может быть некритичным, например, недоступность какого-то хоста.

Критичность в графе

Но в графе от него могут зависеть (в процессе жизни) компоненты с более высокой критичностью.

5.
Профит

Стало

- Поддержке и админам видно все в одном месте
- Оповещаем клиентов автоматически
- Идем дальше – интегрируем UI, в котором работают пользователи

6.
p.s.

Оценить доклад



7.
Спасибо!

Пишите:

- darb@1c.ru



